(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 772 534**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 15836**

(51) Int Cl^6 : **H 04 L 29/10**, H 04 L 29/06, G 06 K 19/073, G 06 F 3/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 15.12.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.06.99 Bulletin 99/24.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *INSIDE TECHNOLOGIES Societe anonyme* — FR.

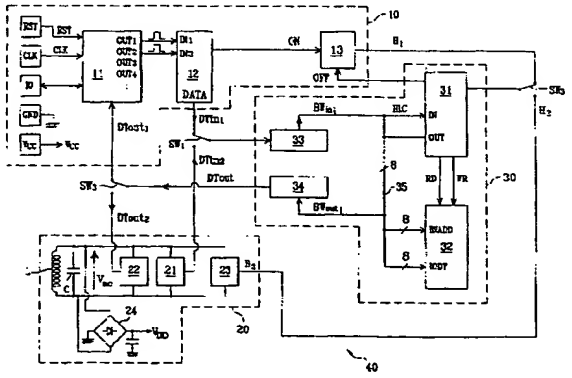
(72) **Inventeur(s) :** PANGAUD NICOLAS.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** MARCHAND ANDRE.

(54) MICROCIRCUIT A LOGIQUE CABLEE COMPORTANT UNE INTERFACE DE COMMUNICATION NUMERIQUE.

(57) La présente invention concerne un microcircuit (40) comprenant un circuit d'interface (11) pour détecter des commandes de bas niveau reçues sous forme de signaux électriques ou de combinaisons de signaux électriques appliqués à des contacts électriques (RST, IO, CLK). Selon l'invention, le microcircuit comprend des moyens (12) pour convertir au moins une première de commande de bas niveau en un bit de valeur 0 et au moins une seconde commande de bas niveau en un bit de valeur 1, de manière à délivrer une chaîne de bits ($DTin_1$) sur réception d'une suite desdites première et seconde commandes de bas niveau. Application: transmission de données binaires à des cartes à mémoire par l'intermédiaire d'une interface de communication de bas niveau ISO 7816-2.



FR 2 772 534 - A1

MICROCIRCUIT A LOGIQUE CABLEE COMPORTANT UNE INTERFACE DE COMMUNICATION NUMERIQUE

La présente invention concerne un microcircuit comprenant un circuit d'interface pour détecter des commandes de bas niveau reçues sous forme de signaux électriques ou de combinaisons de signaux électriques appliqués à des contacts électriques.

La présente invention concerne notamment un microcircuit à logique câblée pour carte à mémoire, prévu pour recevoir des commandes de bas niveau selon la norme ISO 7618-2.

A titre liminaire, on rappellera que le terme générique de "carte à puce" désigne deux grandes catégories de cartes qui se distinguent au plan de la technologie : d'une part, les cartes à microprocesseur, comme les cartes bancaires, d'autre part les cartes dites "à mémoire", par exemple les cartes téléphoniques, les cartes à prépaiement,.... A la différence des cartes à microprocesseur, les cartes à mémoire ne disposent que d'un microcircuit à logique câblée qui offre des possibilités plus réduites qu'un microprocesseur en termes de souplesse d'emploi, de capacité de traitement des données, de programmation... En contrepartie, les microcircuits des cartes à mémoire présentent l'avantage d'être d'une structure plus simple et d'un coût de revient très bas, de sorte qu'ils ont fait l'objet ces dernières années de diverses études ayant conduit à d'importants perfectionnements de leurs fonctions à logique câblée, notamment les fonctions relatives à la sécurité. De tels perfectionnements sont notamment décrits dans les demandes WO 97/14119 et 97/14120 au nom de la demanderesse. Ainsi, aujourd'hui, un microcircuit à

logique câblée de carte à mémoire peut être équipé d'un circuit de cryptographie performant et de moyens de vérification de la validité d'un code secret utilisateur (ou "PIN" code), à la manière d'un microcircuit de carte bancaire.

La diffusion de cartes à mémoire perfectionnées se heurte toutefois au fait qu'à l'heure actuelle, le parc des lecteurs de carte à mémoire en service est essentiellement composé de lecteurs équipés d'une interface de communication assez rudimentaire, répondant à la norme ISO 7816-2. Cette norme, spécifique aux cartes à mémoire, définit en effet un nombre restreint de commandes électriques susceptibles d'être appliquées aux cartes à mémoire par l'intermédiaire de leurs plages de contact. Ces commandes dites de bas niveau sont par exemple :

- WRITE0 : écriture d'un bit à 0 à une adresse de la mémoire spécifiée par un pointeur d'adresse,
- INCRADD : incrémentation d'une unité du pointeur d'adresse de la mémoire,
- RSTADD : remise à 0 du pointeur d'adresse, etc..

Ces commandes sont envoyées sous forme codée au moyen des signaux classiques de remise à zéro RST (Reset) et d'horloge et CLK (Clock). Pour fixer les idées, la figure 1 illustre le codage électrique selon la norme ISO 7816-2 des trois commandes de bas niveau citées plus haut en exemple. La commande WRITE0 est codée par une impulsion du signal RST suivie d'une impulsion d'horloge CLK, la commande INCRADD est codée par une impulsion d'horloge CLK et la commande RSTADD est codée par une impulsion d'horloge CLK émise simultanément à une impulsion du signal RST.

Ces diverses commandes prévues par la norme ISO 7816-2 présentent l'inconvénient de ne permettre que des opérations élémentaires d'écriture, d'effacement ou de

lecture sur la mémoire d'un microcircuit. Aucune commande de haut niveau n'est prévue pour réaliser des opérations plus complexes. Pour réaliser de telles opérations, il est d'usage dans l'art antérieur de prévoir un séquenceur à logique câblé qui déclenche ces opérations à un instant précis de son séquencement, déterminé par le nombre de coups d'horloge CLK reçus depuis la dernière remise à zéro. Par exemple, une opération d'authentification d'une carte à mémoire est réalisée de la façon suivante :

- au moyen de commandes de bas niveau, on enregistre une donnée aléatoire ou ALEA dans la mémoire du microcircuit, par exemple en N coup d'horloge,
- à partir du coup d'horloge N+1, un séquenceur à logique câblée envoie la donnée ALEA dans un circuit de cryptographie et produit, au rythme de l'horloge, un code d'authentification CA et enregistre simultanément ce code dans la mémoire,
- on lit au moyen de commandes de bas niveau le code d'authentification CA enregistré dans la mémoire du microcircuit et on en déduit l'authenticité de la carte.

Cette méthode d'exécution d'opérations complexes au moyen d'un séquenceur, dans laquelle la mémoire intervient pour le transfert des données utiles (par exemple ALEA et CA) en tant que boîte à lettres accessible grâce aux commandes de bas niveau, conduit à réaliser des microcircuits dont le fonctionnement est prédéterminé et figé, ne pouvant pas recevoir des commandes de haut niveau exécutables à tout instant.

Les possibilités restreintes offertes par l'interface ISO 7816-2 représentent également un handicap pour la réalisation d'un microcircuit universel à deux modes de fonctionnement, avec ou sans contact, dont l'architecture générale est décrite dans la demande PCT/FR97/01230 au nom de la demanderesse. Un tel microcircuit permet de réaliser des cartes à mémoire

pouvant être lues aussi bien par des lecteurs de carte sans contact que des lecteurs de cartes à contact conventionnels. En mode de fonctionnement sans contact, le microcircuit reçoit ou émet des données binaires par couplage inductif et peut recevoir, sous forme codée, tous types de commandes de haut niveau. Par contre, en mode contact, le microcircuit ne peut être piloté qu'au moyen des commandes analogiques de bas niveau selon la norme ISO 7816-2. Cette disparité de commandes conduit à prévoir des moyens différents pour l'exécution d'une même opération dans chacun des modes de fonctionnement, et ce type de microcircuit souffre d'une grande complexité et d'un coût de revient élevé.

La présente invention vise à pallier ces divers inconvénients.

Plus particulièrement, un premier objectif de la présente invention est de prévoir un microcircuit à logique câblée pouvant être piloté au moyen de commandes de haut niveau tout en étant compatible avec une interface de communication de bas niveau, par exemple une interface du type ISO 7816-2.

Un autre objectif de la présente invention, indépendant du premier, est de prévoir un microcircuit à deux modes de fonctionnement, avec ou sans contact, offrant la même souplesse de fonctionnement en mode contact qu'en mode sans contact tout en étant d'une structure simple et peu coûteuse.

Pour atteindre ces objectifs, la présente invention propose un procédé pour transmettre des données binaires à un microcircuit comprenant un circuit d'interface agencé pour détecter des commandes de bas niveau reçues sous forme de signaux électriques ou de combinaisons de signaux électriques appliqués à des contacts électriques, comprenant les étapes consistant à : attribuer par convention la valeur logique 0 à au moins une première

commande de bas niveau et la valeur logique 1 à au moins une deuxième commande de bas niveau ; appliquer au microcircuit une succession des première et deuxième commandes ; dans le microcircuit, convertir chaque commande de bas niveau reçue par sa valeur binaire attribuée par convention, de manière à transformer une suite des première et seconde commandes de bas niveau en une chaîne de bits.

Grâce à ce procédé, on peut créer un canal de communication numérique avec le microcircuit tout en assurant une compatibilité du canal de communication avec les caractéristiques de l'interface et le matériel de gestion de cette interface. Avantageusement, ce procédé est appliqué à la transmission au microcircuit de commandes de haut niveau codées sous forme binaire.

Selon un mode de réalisation, on utilise une troisième commande de bas niveau comme moyen de séparation de mots binaires dans une chaîne de bits.

Selon un mode de réalisation, la première commande de bas niveau est une commande d'écriture d'un bit à 0 dans une mémoire ; la deuxième commande de bas niveau est une commande d'incrémentation d'une adresse de lecture ou d'écriture dans une mémoire ; la troisième commande de bas niveau, optionnelle, est une commande de remise à zéro d'une adresse de lecture ou d'écriture dans une mémoire.

La présente invention concerne également un microcircuit comprenant un circuit d'interface agencé pour détecter des commandes de bas niveau reçues sous forme de signaux électriques ou de combinaisons de signaux électriques appliqués à des contacts électriques, comprenant des moyens de conversion binaire de commandes de bas niveaux reçues par le circuit d'interface, agencés pour convertir au moins une première commande de bas niveau en un bit de valeur 0 et au moins une seconde

commande de bas niveau en un bit de valeur 1, de manière à délivrer une chaîne de bits sur réception d'une suite des première et seconde commandes de bas niveau.

Selon un mode de réalisation, le microcircuit comprend des moyens pour fractionner en un ou plusieurs mots binaires de longueur prédéterminée une chaîne de bits délivrée par les moyens de conversion.

Selon un mode de réalisation, les moyens de conversion sont agencés pour convertir au moins une troisième commande de bas niveau en un signal de séparation de mots binaires dans une chaîne de bits.

Selon un mode de réalisation, le microcircuit comprend des moyens pour convertir en données parallèles des mots binaires contenus dans une chaîne de bits délivrée par les moyens de conversion.

Selon un mode de réalisation, le microcircuit comprend des moyens pour insérer un bit de séparation de mots binaires dans une chaîne de bits.

Selon un mode de réalisation, le microcircuit comprend une unité de traitement pour exécuter des commandes délivrées sous forme binaire par les moyens de conversion.

Selon un mode de réalisation, l'unité de traitement est agencée pour exécuter des commandes complexes comportant plusieurs champs.

Selon un mode de réalisation, le microcircuit comprend un circuit d'interface agencé pour détecter des commandes de bas niveau codées selon la norme ISO 7816-2.

La présente invention s'applique notamment à un microcircuit à deux modes de fonctionnement, avec ou sans contact, comprenant des moyens pour recevoir des données binaires en mode de fonctionnement sans contact.

Selon l'invention, le microcircuit comprend une partie commune pour le traitement de données binaires

reçues dans l'un quelconque des deux modes de fonctionnement.

Ces objets, caractéristiques et avantages de la présente invention, ainsi que d'autres, seront exposés plus en détail dans la description suivante du procédé de l'invention et d'un microcircuit à deux modes de fonctionnement mettant en oeuvre ce procédé, en relation avec les figures jointes parmi lesquelles :

- la figure 1 précédemment décrite représente le codage électrique de commandes de bas niveau selon la norme ISO 7816-2,
- la figure 2 représente sous forme de blocs le schéma électrique d'un microcircuit à deux modes de fonctionnement selon l'invention, et
- la figure 3 illustre un mode de réalisation particulier de certains éléments du microcircuit de la figure 2.

Description de l'invention

La figure 2 représente le schéma électrique d'un microcircuit 40 à logique câblée selon l'invention, destiné à être monté sur une carte plastique pour former une carte à mémoire. Le microcircuit 40 est du type décrit dans la demande PCT/FR97/01230 et présente deux modes de fonctionnement, avec ou sans contact. Le microcircuit 40 comprend ainsi une partie 10 spécifique à la gestion d'une communication en mode contact, une partie 20 spécifique à la gestion d'une communication en mode sans contact, et une partie 30 commune aux deux modes de fonctionnements.

Selon l'invention, le microcircuit 40 présente trois caractéristiques distinctes qui seront décrites en détail par la suite :

1) la partie 10 du mode contact dispose d'un canal de communication numérique tout en étant compatible avec la norme ISO 7816-2,

2) ce canal de communication numérique est utilisé pour envoyer au microcircuit, en mode contact, des commandes de haut niveau codées en binaire,

3) la partie commune 30 traite indifféremment des commandes de haut niveau reçues en mode contact et des commandes de haut niveau reçues en mode sans contact.

On décrira tout d'abord la structure de la partie 10 spécifique au mode de fonctionnement à contact.

1/ Partie spécifique au mode fonctionnement à contact

La partie 10 comprend de façon classique un contact RST pour recevoir un signal de remise à zéro RST, un contact CLK pour recevoir un signal d'horloge externe CLK, un contact IO pour recevoir des données d'entrée/sortie, un contact GND de masse et un contact VCC pour recevoir une tension VCC d'alimentation du microcircuit 40 lorsque celui-ci fonctionne en mode contact, ces divers contacts étant prévus par la norme ISO 7816-2. La partie 10 comprend également de façon classique un circuit d'interface 11 conforme à cette norme, par exemple le circuit SLE4403 commercialisé par la société SIEMENS. Le circuit d'interface 11 est connecté aux contacts RST, CLK, IO et est agencé pour détecter les commandes de bas niveau LC_1, LC_2, LC_3, LC_4... appliquées au microcircuit 40. Le circuit 11 comporte une pluralité de sorties OUT_1, OUT_2, OUT_3, OUT_4... , chaque sortie étant associée à une commande de bas niveau LC_1, LC_2, LC_3, LC_4..., et délivre une impulsion de tension sur une sortie OUT_i lorsque la commande LC_i correspondante est détectée.

Selon l'invention, la partie 10 comprend également un convertisseur 12 connecté à au moins deux sorties du circuit 11, ici les sorties OUT_1, OUT_2, et comportant une sortie numérique DATA. Ce convertisseur 12 est agencé pour convertir en données binaires au moins deux commandes de bas niveau, ici LC_1, LC_2, reçues par le

circuit d'interface 11, utilisées pour transmettre les valeurs binaires 0 et 1. Ainsi, le convertisseur 12 délivre sur sa sortie DATA un bit à 0 quand la commande LC_1 est détectée (une impulsion de tension étant émise par la sortie OUT_1) et délivre un bit à 1 quand la commande LC_2 est détectée (une impulsion de tension étant émise par la sortie OUT_2). Dans un souci de simplicité, on ne décrira pas la structure interne du convertisseur 12 dont la réalisation au moyen de portes logiques et de bascules est à la portée de l'homme de l'art.

Ainsi, lorsque le microcircuit 40 reçoit une suite de commandes de bas niveau LC_1, LC_2, la sortie DATA du convertisseur 12 délivre une suite ou chaîne de bits $DTin_1$. Par exemple, la suite de commandes suivante:

LC_1, LC_2, LC_2, LC_1, LC_1, LC_2, LC_1, LC_2,

est convertie en une chaîne de bits égale à :

0 1 1 0 0 1 0 1

En d'autres termes, les commandes de bas niveau LC_1, LC_2 choisies pour le transfert de données binaires au microcircuit 40 sont détournées de leur fonction première. Ces commandes ne produisent aucun autre effet sur le microcircuit, et ne sont pas exécutées.

Ainsi, l'application au microcircuit d'une suite ininterrompue de commandes de bas niveau LC_1, LC_2 permet avantageusement de créer un canal de communication numérique. Selon un autre aspect de l'invention, ce canal de communication est utilisé pour transmettre au microcircuit des commandes de haut niveau codées en binaire dont des exemples seront décrits plus loin.

Par ailleurs, l'émission de données binaires DTout1 par la partie 10 est faite de façon classique en

appliquant ces données sur le contact IO en synchronisation avec le signal d'horloge externe CLK, cette opération étant réalisée par l'intermédiaire du circuit d'interface 11 qui assure la synchronisation du transfert de données avec l'horloge CLK.

Enfin, la partie 10 comprend un générateur 13 d'un signal d'horloge interne H1 propre au mode de fonctionnement à contact, de fréquence supérieure au signal d'horloge externe CLK. Le générateur 13 est activé par un signal ON délivré par le convertisseur 12 dès l'instant où celui-ci émet une donnée sur sa sortie DATA, et est désactivé par un signal OFF délivré par une unité de traitement 31 qui sera décrite plus loin.

2/ Partie spécifique au mode de fonctionnement sans contact

La partie 20 spécifique au fonctionnement sans contact est en elle-même classique et ne sera décrite que succinctement, à titre d'exemple. La partie 20 comprend une interface de communication sans contact comprenant une bobine d'antenne L et une capacité C, l'ensemble formant un circuit d'antenne résonant LC de fréquence propre Fp. La partie 20 comprend par ailleurs un circuit démodulateur-décodeur 21, un circuit codeur-modulateur 22, un circuit 23 délivrant le signal d'horloge interne H2 du mode sans contact, et un pont redresseur 24 à diodes, ces divers circuits étant connectés aux bornes du circuit d'antenne LC.

En présence d'un champ magnétique oscillant à la fréquence Fp, émis par exemple par la bobine d'un lecteur de carte sans contact (non représenté), la bobine L délivre une tension alternative induite Vac. Cette tension Vac est transformée par le pont redresseur 24 en une tension continue VDD assurant l'alimentation du microcircuit 40 en mode de fonctionnement sans contact. La réception de données binaires $DTin_2$ est assurée par le

circuit 21 qui démodule la tension Vac et délivre ces données binaires $DTin_2$. L'émission de données binaires DTout2 est assurée par le circuit 22 qui module la charge de la bobine L en fonction de ces données, selon un codage prédéterminé. Cette modulation de charge se répercute par couplage inductif sur la bobine du lecteur de carte qui peut ainsi en déduire les données DTout2 qui lui sont envoyées. Enfin, le signal d'horloge H2 du mode sans contact est de façon classique extrait de la tension Vac par le circuit 23, par exemple par division de fréquence, sa fréquence étant généralement un sous-multiple de la fréquence Fp.

Comme on l'a déjà indiqué, ces divers circuits sont bien connus de l'homme de l'art et ne seront pas décrits plus en détail. De plus, l'émission et la réception de données binaires par la partie 20 peuvent reposer sur d'autres techniques que la modulation d'amplitude de la tension Vac et la modulation de la charge de la bobine L, par exemple la modulation FSK, la transmission de signaux infrarouges au moyen de composants optoélectroniques, etc.

3/ Partie commune aux deux modes de fonctionnement

La partie 30, essentiellement numérique, comprend une unité de traitement 31, une mémoire de donnée 32, un tampon d'entrée 33 et un tampon de sortie 34 ayant ici une capacité de huit bits chacun. La mémoire 32 comporte une entrée d'adresse INADD, un port d'entrée/sortie parallèle IODT, et est pilotée par des signaux WR (écriture) et RD (lecture) délivrés par l'unité de traitement 31. Le tampon 33 est un registre à décalage comportant une entrée série et une sortie parallèle et le tampon 34 est un registre à décalage comportant une entrée parallèle et une sortie série. Un commutateur SW1 à deux positions permet d'appliquer à l'entrée du tampon 33 des données binaires $DTin_1$ délivrées par le

convertisseur 12 de la partie 10 ou des données binaires $DTin_2$ délivrées par le circuit démodulateur-décodeur 21 de la partie 20. La sortie parallèle du tampon 33 est connectée à un bus interne 35, ici de huit bits. Le bus 35 est connecté à une entrée IN et une sortie OUT de l'unité de traitement 31, à l'entrée INADD et au port IODT de la mémoire 32, ainsi qu'à l'entrée parallèle du tampon 34. La sortie du tampon 34 délivre des données DTout qui peuvent être appliquées au circuit d'interface 11 de la partie 10 ou au circuit codeur-modulateur 22 de la partie 20, par l'intermédiaire d'un commutateur SW2 à deux positions.

L'unité de traitement 31 est une machine d'états à nombre d'états finis d'un type connu en soi dont la réalisation est à la portée de l'homme de l'art, agencée pour décoder et exécuter des commandes de haut niveau codées en binaire. L'unité de traitement 31 comprend divers circuits classiques nécessaires à l'exécution de ces commandes de haut niveau, par exemple un circuit de décodage des commandes, un circuit de cryptographie à logique câblée et un circuit de contrôle de signatures numériques. L'activation de l'unité de traitement 31 est assurée par l'un des deux signaux d'horloge H1 ou H2 décrits plus haut, sélectionné en fonction du mode de fonctionnement du microcircuit au moyen d'un commutateur à deux positions SW3.

4/ Fonctionnement et avantages du microcircuit

Les données $DTin_1$ ou $DTin_2$ reçues sous forme série sont injectées dans le tampon d'entrée 33 de la partie 30, et le contenu du tampon 33 est déchargé en parallèle sur le bus 35 tous les huit bits reçus, sous la forme d'un mot binaire $BWin_i$. Selon l'invention, ce mot binaire $BWin_i$ est une commande de haut niveau ou un élément d'une commande plus complexe, par exemple :

- un code opération $CODE_{OP}$ d'une opération à exécuter, à appliquer sur l'entrée IN de l'unité de traitement 31,
- une adresse ADD à appliquer sur l'entrée INADD de la mémoire 32,
- une donnée WDATA à enregistrer dans la mémoire 32, par l'intermédiaire du port IODT,
- une donnée aléatoire ALEA à partir de laquelle le microcircuit 40 doit produire un code d'authentification CA,
- une signature CRC de message, permettant de détecter les erreurs de transmission, etc.

Les commandes de haut niveau, les codes opérations $CODE_{OP}$, les données du type ALEA ou CRC sont lues et traitées par l'unité de traitement 31. Les autres données comme des adresses ADD ou des données WDATA à enregistrer sont directement appliquées à la mémoire 32, sous le contrôle de l'unité 31.

Par ailleurs, les données DTout1, DTout2 devant être envoyées à un lecteur de carte sont appliquées en parallèle, sous forme de mots binaires $BWout_i$, à l'entrée du tampon de sortie 34 et délivrées bit à bit par la sortie du tampon 34. Ces données peuvent comprendre, par exemple :

- un code INF délivré par l'unité de traitement 31,
- un code d'authentification CA délivré par l'unité 31,
- une donnée RDATA lue dans la mémoire 32,
- une donnée WDATA écrite dans la mémoire 32, renvoyée pour confirmation, etc.

Ces données DTout sont envoyées au circuit 11 de la partie 10 ou au circuit codeur-modulateur 22 de la partie 20, selon la position du commutateur SW2.

Ainsi, avantageusement, le microcircuit 40 reçoit des commandes de haut niveau de même format et de même codage quel que soit son mode de fonctionnement. Cet avantage est obtenu grâce à la possibilité de recevoir

des données binaires en mode contact, et par le fait que le microcircuit ne comporte qu'un seul circuit de traitement 31 pour les deux modes de fonctionnement. Cette caractéristique simplifie considérablement la structure du microcircuit et permet d'obtenir la même souplesse de fonctionnement en mode contact qu'en mode sans contact.

5/ Exemple de commandes de haut niveau envoyées au microcircuit

Pour fixer les idées, on trouvera ci-après quelques exemples de commandes de haut niveau pouvant être envoyées au microcircuit 40. Ces commandes sont divisées en champs de huit bits se retrouvant dans le microcircuit 40 sous forme de mots binaires $BWin_i$ délivrés par le tampon 33 sur le bus 35. Le premier champ $CODE_{OP}$ contient le code de l'opération à exécuter et les autres champs contiennent des données complémentaires et/ou des données de signature.

Commande READ (lecture de la mémoire 32) :

$CODE_{READ}$	ADD	CRC_1	CRC_2

Cette commande comprend le code de l'opération $CODE_{READ}$, une adresse de lecture ADD, et deux octets de signature CRC_1, CRC_2 formant ensemble une signature sur 16 bits.

Commande WRITE (écriture dans la mémoire 32) :

$CODE_{WRITE}$	ADD	W_1	W_2	W_3	W_4	CRC_1	CRC_2

Cette commande comprend le code de l'opération $CODE_{WRITE}$, une adresse d'écriture ADD, une donnée de 32 bits à écrire dans la mémoire, décomposée en quatre octets W_1 à W_4, et deux octets de signature CRC_1, CRC_2.

Commande AUTHENTICATE (demande d'authentification)

$CODE_{AUTH}$	$ALEA_1$	$ALEA_2$	$ALEA_3$	$ALEA_4$

Cette commande d'authentification du microcircuit comprend le code de l'opération $CODE_{AUTH}$ et une donnée aléatoire de 32 bits décomposée en quatre octets $ALEA_1$ à $ALEA_4$.

Comme on l'a déjà indiqué, l'émission des réponses du microcircuit 40 en mode contact est faite de façon plus conventionnelle, par l'intermédiaire du contact IO et en synchronisation avec l'horloge externe CLK, conformément à la norme ISO 7816-2. Le format des réponses peut être uniformisé pour les deux modes de fonctionnement, et est par exemple le suivant :

INF	XDATA	CRC

Le champ INF peut être une donnée invariable commune à tous les messages, où une donnée variable permettant de coder des messages en retour. Le champ XDATA contient une information à transmettre, par exemple une donnée RDATA ou WDATA, un code d'authentification CA, etc. Enfin, le champ de vérification CRC est optionnel et peut être utile dans des messages de confirmation au moyen desquels le microcircuit 40 confirme l'exécution d'une opération nécessitant un haut niveau de contrôle et de sécurité.

6/ Envoi des commandes de haut niveau en mode contact à partir d'un lecteur de carte de type classique

Dans ce qui précède on s'est attaché à décrire la mise en oeuvre, du côté du microcircuit 40, du procédé selon l'invention permettant de recevoir des données binaires par l'intermédiaire de commandes de bas niveau. La mise en oeuvre de l'invention suppose par ailleurs que

l'on soit en mesure, du côté d'un lecteur de carte, d'émettre d'une façon simple les commandes de bas niveau LC_1, LC_2 véhiculant les données binaires. Ici, la présente invention se fonde sur le fait que, façon classique, les lecteurs de carte à mémoire sont programmables au moyen de macro-commandes standardisées facilitant le travail des programmeurs. Ces macro-commandes sont décomposées automatiquement par les lecteurs de cartes en une suite de commandes de bas niveau.

Plus particulièrement, l'idée de l'invention est d'envoyer au microcircuit 40 les octets $BWin_i$ d'une commande de haut niveau au moyen de la macro-commande classique :

$$WRITE("octet"_h, "adresse"_h)$$

qui signifie : "écrire l'octet spécifié (en hexadécimal) à l'adresse spécifiée (également en hexadécimal)", chaque octet $BWin_i$ à envoyer étant placé dans le champ "octet". Cette macro-commande est décomposée par les lecteurs de carte en une suite de commandes de bas niveau WRITE0 (écriture d'un bit à 0) et INCRADD (incrémentation d'un pointeur d'adresse) déjà décrites au préambule, la commande WRITE0 étant émise lorsque un 0 doit être écrit dans une mémoire, et la commande INCRADD émise lorsqu'un 1 doit y être écrit (en effet, l'écriture d'un bit à 1 dans une mémoire de carte à mémoire se traduit en pratique par une simple incrémentation d'adresse au moyen de la commande de bas niveau INCRADD, tous les points mémoire étant mis à 1 à la mise en service de la carte).

Dans le cas où la macro-commande WRITE est utilisée, comme on vient de le proposer, les commandes de bas niveau LC_1 et LC_2 véhiculant des données numériques sont alors WRITE0 et INCRADD.

En pratique, la présente invention propose d'envoyer chaque mot binaire $BWin_i$ exprimé en hexadécimal au moyen de la macro-commande suivante :

$$WRITE(BWin_i, 00_h)$$

dans laquelle le champ "adresse" est toujours à zéro. En procédant ainsi, on évite que le lecteur de carte n'envoie, avant la suite de commandes WRITE0 (écriture d'un 0) et INCRADD (écriture d'un 1), une suite de commandes préliminaires INCRADD ayant pour but d'amener un pointeur d'adresse à l'adresse spécifiée dans l'instruction. Ainsi, par exemple, le mot :

$BWin_i$ = 0 1 1 0 0 1 0 1 (soit 65_h en notation hexadécimale)

est envoyé au moyen de la macro-commande :

WRITE (65_h, 00_h)

Cette macro-commande provoque dans un lecteur de carte à mémoire l'émission de la suite de commandes de bas niveau suivante :

RSTADD, WRITE0, INCRADD, INCRADD, WRITE0, WRITE0, INCRADD, WRITE0, INCRADD

La commande RSTADD (remise à 0 du pointeur d'adresse) n'étant pas reconnue par le convertisseur 12 comme une valeur binaire, cette suite de commandes est elle-même transformée par le convertisseur 12 en une chaîne de bits égale à :

0 1 1 0 0 1 0 1

En définitive, et très avantageusement, on retrouve sur la sortie DATA du convertisseur 12 le mot binaire $BWin_i$ placé dans la macro-commande.

Par ailleurs, la réception de données du type INF, XDATA et CRC par un lecteur de carte peut être obtenue grâce à la macro-commande classique :

$$READ\ (N_h,\ 00_h)$$

dans laquelle N exprimé en hexadécimal est le nombre de bits que l'on s'attend à recevoir du microcircuit 40, le champ adresse étant toujours mis à zéro pour la raison susmentionnée. Bien entendu, cette macro-commande n'est pas perçue comme une commande par le microcircuit 40. Cette macro-commande génère simplement l'émission de N coups d'horloge externe CLK. Dans le microcircuit 40 selon l'invention, l'unité de traitement 31 sait qu'elle va devoir émettre des données (par exemple parce qu'elle a reçue précédemment une commande de haut niveau READ ou AUTHENTICATE), et attend le signal d'horloge CLK. Lorsque le premier coup d'horloge CLK est reçu, l'unité 31 envoie ces données bit à bit sur le contact IO, par l'intermédiaire du circuit d'interface 11, en synchronisation avec l'horloge CLK conformément à la norme ISO 7816-2.

7/ Insertion d'un bit de séparation dans les commandes de haut niveau envoyés au microcircuit

Dans ce qui précède, on a vu que les commandes de haut niveau envoyées au microcircuit 40 comportent plusieurs champs $CODE_{OP}$, ALEA, W_i,... se retrouvant sous la forme d'une chaîne de bits sur la sortie DATA du convertisseur 12, puis sous la forme de mots binaires $BWin_i$ sur le bus interne 35, la taille des champs étant adaptée à la capacité du tampon d'entrée 33, ici de huit

bits. En pratique, il est donc nécessaire de prévoir un moyen pour déclencher le déchargement du tampon 33 sur le bus 35, à chaque fois que celui-ci est plein. Un comptage des impulsions délivrées par les sorties OUT1, OUT2 du circuit d'interface 11 est envisageable mais s'avère être une solution médiocre pouvant conduire à des erreurs de synchronisation. La présente invention propose une méthode plus avantageuse, qui consiste à :

1) insérer un bit de séparation BS, ou bit de "start", à l'entrée du tampon 33 avant l'arrivée des bits significatifs d'une commande,

2) propager le bit BS dans le tampon 33 à chaque insertion d'un bit significatif,

3) décharger le tampon 33 quand le bit BS apparaît à l'autre extrémité du tampon 33.

Pour mettre en oeuvre cette méthode, il est par ailleurs avantageux de générer le bit de séparation BS au moyen de la commande de bas niveau RSTADD. En effet, on a vu plus haut que l'exécution de la macro-commande WRITE($BWin_i$, 00_h) dans laquelle le champ "adresse" est à zéro, commence toujours par l'envoi de la commande RSTADD visant à remettre à zéro un pointeur d'adresse.

La figure 3 représente un mode de réalisation du convertisseur 12 et du tampon d'entrée 33 mettant en oeuvre la méthode qui vient d'être décrite. Le convertisseur 12 est maintenant connecté à trois sorties OUT_1, OUT_2, OUT_3 du circuit 11, activées respectivement par les commandes de bas niveau WRITE0, INCRADD, et RSTADD. Le tampon 12 comporte neuf cellules mémoire CEL_1 à CEL_9 en cascade, la sortie DATA du convertisseur 12 étant connectée à l'entrée de la première cellule CEL_1. Le décalage des bits des cellules CEL_i vers les cellules de rang supérieur CEL_{i+1} est déclenché par un signal SHIFT délivré par le convertisseur 12. Par ailleurs, le contenu des cellules CEL_1 à CEL_8 est déchargé sur le bus

décalages déclenchés par le signal SHIFT, le bit BS se trouve à la sortie de la cellule CEL_9 de sorte que le signal de déchargement LTCH passe à 0. Ainsi, selon l'invention, l'insertion du bit de séparation BS dans la chaîne binaire délivrée par le convertisseur 12 permet de décharger automatiquement le tampon 33 sur le bus 35 et par ailleurs d'assurer une bonne synchronisation entre le microcircuit 40 et un lecteur de carte à mémoire.

8/ Variantes et applications de l'invention

Il va de soi que les aspects de la présente invention relatifs à la transmission de données binaires par l'intermédiaire d'une interface ISO 7816-2 sont applicables aussi bien aux microcircuits à deux modes de fonctionnement qu'aux microcircuits fonctionnant exclusivement en mode contact. Ainsi, la présente invention permet non seulement la réalisation d'un microcircuit à deux modes de fonctionnement de conception simple, rationnelle, offrant une grande souplesse d'utilisation, qu'un microcircuit exclusivement à contact, offrant également une grande souplesse d'utilisation par son aptitude à recevoir des commandes de haut niveau. Par ailleurs, il entre dans le cadre de l'invention d'appliquer par analogie l'enseignement qui vient d'être donné à des interfaces normalisées de bas niveau autres que l'interface ISO 7816-2 pour cartes à mémoire. L'invention est donc applicable à tout type de microcircuit monté sur un support portable et piloté par l'intermédiaire d'une interface de bas niveau imposée par une norme.

Egalement, il apparaîtra clairement à l'homme de l'art que certaines caractéristiques de l'invention, comme le fait de procéder à une transformation série/parallèle des données binaires reçues, ne sont pas impératives à la mise en oeuvre de l'invention. Il est par exemple envisageable de réaliser un microcircuit

comprenant une mémoire à port d'entrée/sortie série. De façon générale, diverses architectures de circuits connues de l'homme de l'art peuvent donc être mises en oeuvre dans un microcircuit selon l'invention.

Enfin, il convient de noter qu'en pratique le circuit d'interface 11 et le convertisseur 12 selon l'invention peut être fusionnés en un seul circuit dont la fonction est de détecter des signaux ou combinaisons de signaux reçus et délivrer les valeurs binaires correspondantes.

REVENDICATIONS

1. Microcircuit (40) comprenant un circuit d'interface (11) agencé pour détecter des commandes de bas niveau (LC_1, LC_2, WRITE0, INCRADD, RSTADD) reçues sous forme de signaux électriques (RST, CLK, IO) ou de combinaisons de signaux électriques (RST, CLK, IO) appliqués à des contacts électriques, caractérisé en ce qu'il comprend des moyens (12) de conversion binaire de commandes de bas niveaux (LC_1, LC_2, WRITE0, INCRADD, RSTADD) reçues par le circuit d'interface (11), agencés pour convertir au moins une première commande de bas niveau (LC_1, WRITE0, RSTADD) en un bit de valeur 0 et au moins une seconde commande de bas niveau (LC_2, INCRADD) en un bit de valeur 1, de manière à délivrer une chaîne de bits ($DTin_1$) sur réception d'une suite desdites première (LC_1, WRITE0, RSTADD) et seconde (LC_2, INCRADD) commandes de bas niveau.

2. Microcircuit selon la revendication 1, comprenant des moyens (12, 33, BS) pour fractionner en un ou plusieurs mots binaires ($BWin_i$) de longueur prédéterminée une chaîne de bits ($DTin_1$) délivrée par les moyens de conversion (12).

3. Microcircuit selon l'une des revendications 1 et 2, dans lequel les moyens de conversion (12) sont agencés pour convertir au moins une troisième commande (RSTADD) de bas niveau en un signal (BS) de séparation de mots binaires ($BWin_i$) dans une chaîne de bits ($DTin_1$).

4. Microcircuit selon l'une des revendications 1 à 3, comprenant des moyens (33) pour convertir en données parallèles des mots binaires ($BWin_i$) contenus dans une chaîne de bits ($DTin_1$) délivrée par les moyens de conversion (12).

5. Microcircuit selon l'une des revendications 1 à 4, comprenant des moyens (12) pour insérer un bit (BS) de séparation de mots binaires ($BWin_i$) dans une chaîne de bits ($DTin_1$).

6. Microcircuit selon l'une des revendications 1 à 5, comprenant une unité de traitement (31) pour exécuter des commandes (WRITE, AUTHENT, READ) délivrées sous forme binaire par les moyens de conversion (12).

7. Microcircuit selon la revendication 6, dans lequel l'unité de traitement (31) est agencée pour exécuter des commandes complexes (WRITE, AUTHENT, READ) comportant plusieurs champs ($CODE_{OP}$, ADD, ALEA, CRC, W_i).

8. Microcircuit selon l'une des revendications précédentes, comprenant un circuit d'interface (11) agencé pour détecter des commandes de bas niveau (LC_1, LC_2, WRITE0, INCRADD, RSTADD) codées selon la norme ISO 7816-2.

9. Microcircuit selon la revendication 8, dans lequel ladite première commande de bas niveau (LC_1, WRITE0) est une commande d'écriture d'un bit à 0 dans une mémoire.

10. Microcircuit selon l'une des revendications 8 et 9, dans lequel ladite deuxième commande de bas niveau (LC_2, INCRADD) est une commande d'incrémentation d'une adresse de lecture ou d'écriture dans une mémoire.

11. Microcircuit selon l'une des revendications 8 à 10 dans lequel ladite troisième commande de bas niveau (RSTADD) est une commande de remise à 0 d'une adresse de lecture ou d'écriture dans une mémoire.

12. Microcircuit selon l'une des revendications précédentes, à deux modes de fonctionnement, avec ou sans contact, comprenant des moyens (20) pour recevoir des données binaires ($DTin_2$) en mode de fonctionnement sans contact.

13. Microcircuit selon la revendication 12, comprenant une partie commune (30) pour le traitement de données binaires ($DTin_1$, $DTin_2$) reçues dans l'un quelconque des deux modes de fonctionnement.

14. Procédé pour transmettre des données binaires à un microcircuit (40) comprenant un circuit d'interface (11) agencé pour détecter des commandes de bas niveau (LC_1, WRITE0, LC_2, INCRADD, RSTADD) reçues sous forme de signaux électriques (RST, CLK, IO) ou de combinaisons de signaux électriques (RST, CLK, IO) appliqués à des contacts électriques, caractérisé en ce qu'il comprend les étapes consistant à :

- attribuer par convention la valeur logique 0 à au moins une première commande de bas niveau (LC_1, WRITE0, RSTADD) et la valeur logique 1 à au moins une deuxième commande de bas niveau (LC_2, INCRADD),
- appliquer au microcircuit (40) une succession desdites première et deuxième commandes (LC_1, LC_2, WRITE0, INCRADD, RSTADD),
- dans le microcircuit (40), convertir (12) chaque commande de bas niveau (LC_1, LC_2, WRITE0, INCRADD, RSTADD) reçue par sa valeur binaire attribuée par convention, de manière à transformer une suite desdites première (LC_1, WRITE0, RSTADD) et seconde (LC_2, INCRADD) commandes de bas niveau en une chaîne de bits ($DTin_1$).

15. Procédé selon la revendication 14, dans lequel on utilise une troisième commande de bas niveau (RSTADD) comme moyen de séparation de mots binaires ($BWin_i$) dans une chaîne de bits ($DTin_1$).

16. Procédé selon l'une des revendications 14 et 15, appliqué à la transmission de commandes de haut niveau (WRITE, AUTHENT, READ) codées sous forme binaire.

17. Procédé selon l'une des revendications 14 à 16, dans lequel lesdites commandes de bas niveau sont définies par la norme ISO 7816-1.

18. Procédé selon la revendication 17, dans lequel ladite première commande de bas niveau (LC_1, WRITE0) est une commande d'écriture d'un bit à 0 dans une mémoire.

19. Procédé selon l'une des revendications 17 et 18, dans lequel ladite deuxième commande de bas niveau (LC_2, INCRADD) est une commande d'incrémentation d'une adresse de lecture ou d'écriture dans une mémoire.

20. Procédé selon l'une des revendications 17 à 19, dans lequel ladite troisième commande de bas niveau (RSTADD) est une commande de remise à zéro d'une adresse de lecture ou d'écriture dans une mémoire.

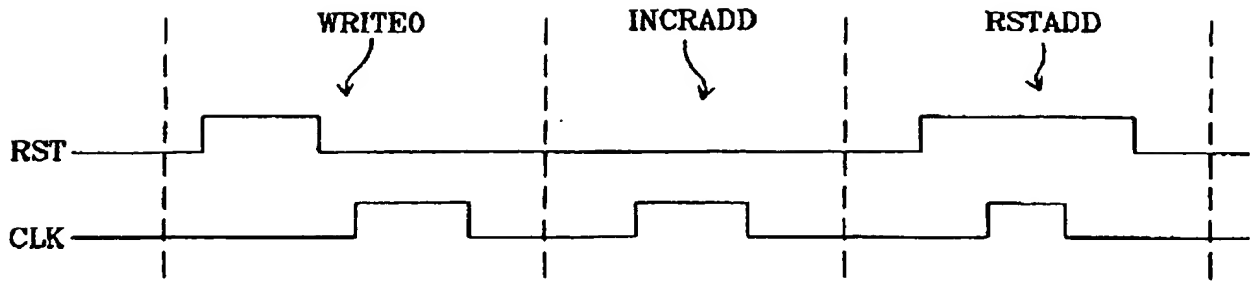

WRITE0
INCRADD
RSTADD
RST
CLK

FIG.1

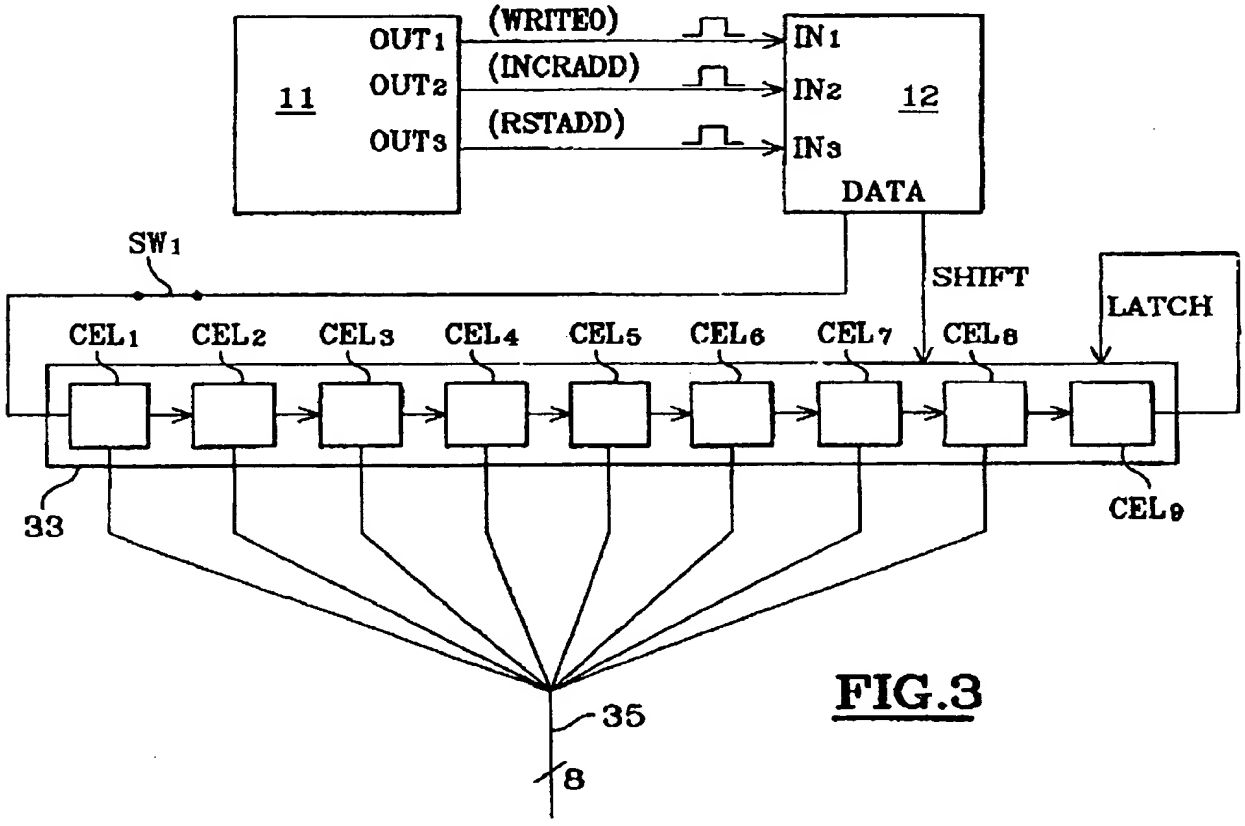

OUT1
OUT2
OUT3
11
(WRITE0)
(INCRADD)
(RSTADD)
IN1
IN2
IN3
12
DATA
SW1
SHIFT
LATCH
CEL1
CEL2
CEL3
CEL4
CEL5
CEL6
CEL7
CEL8
CEL9
33
35
8

FIG.3

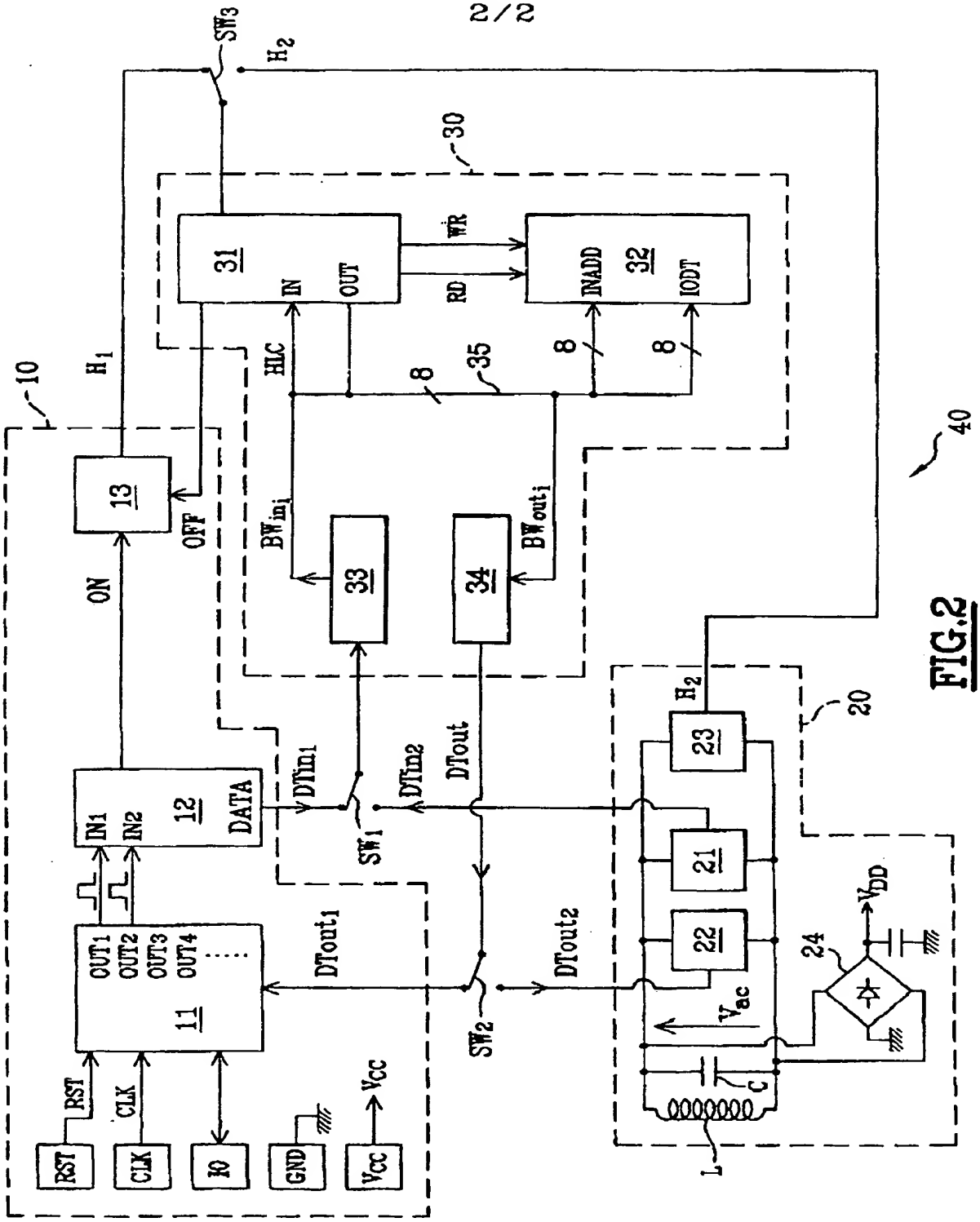

SW3
H2
30
31
IN
OUT
WR
RD
32
INADD
IODT
HLC
8
35
8
8
H1
10
13
ON
OFF
BWini
BWouti
33
34
40
IN1
IN2
12
DATA
DTin1
DTin2
DTout
SW1
H2
23
20
21
22
24
VDD
OUT1
OUT2
OUT3
OUT4
11
DTout1
DTout2
SW2
Vac
C
L
RST
CLK
I/O
GND
Vcc

FIG.2

REPUBLIQUE FRANÇAISE

2772534

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 553685
FR 9715836

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
D,A	WO 97 14119 A (INSIDE TECHNOLOGIES ;KOWALSKI JACEK (FR)) 17 avril 1997 * page 8, ligne 27 - page 17, ligne 32; figures 1,2 *	1-20
A	FR 2 698 195 A (GEMPLUS CARD INT) 20 mai 1994 * abrégé *	1,14

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G06K

Date d'achèvement de la recherche: 30 octobre 1998

Examinateur: Degraeve, A

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

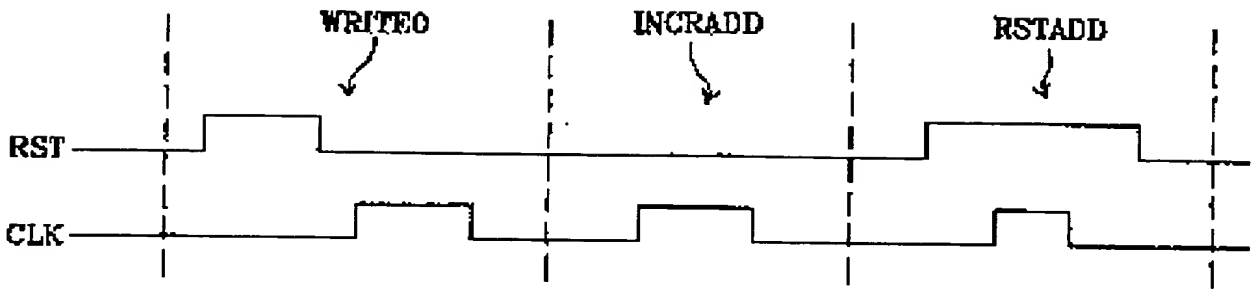


FIG.1

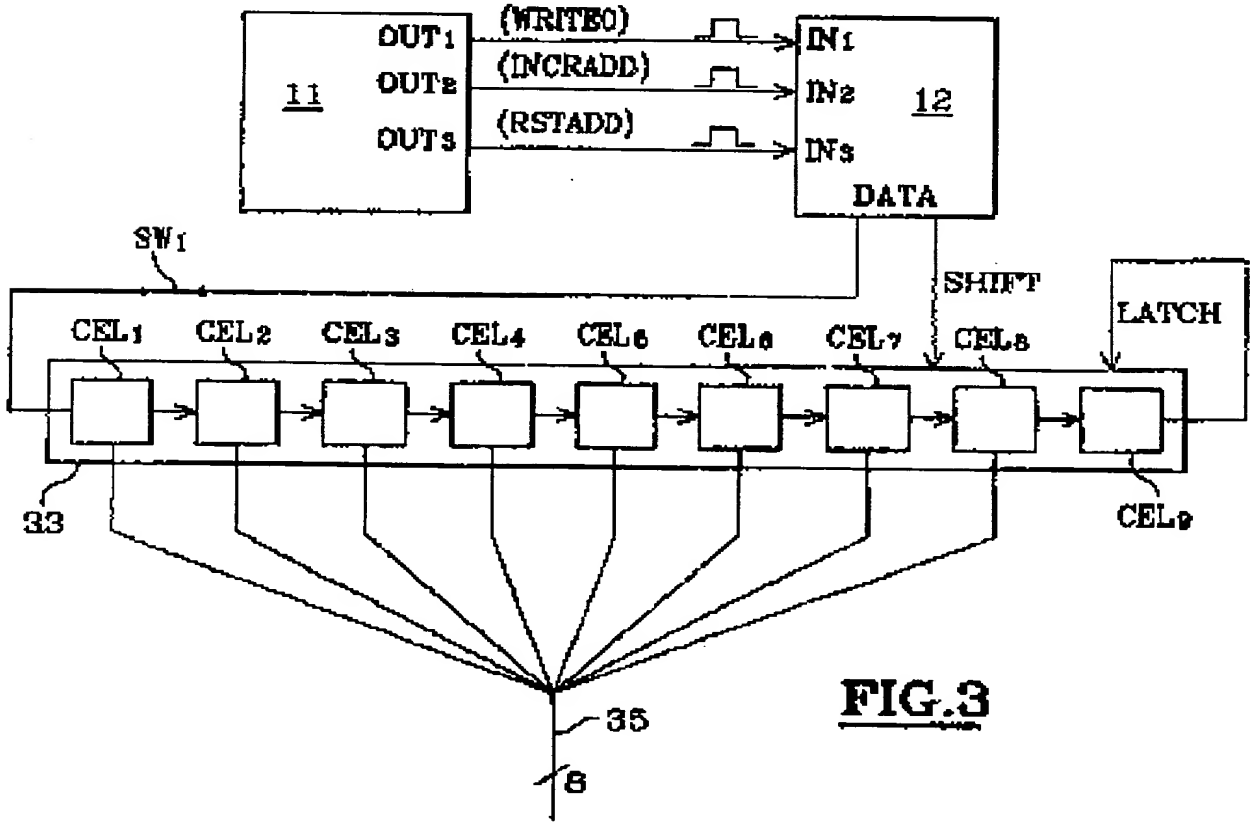


FIG.3

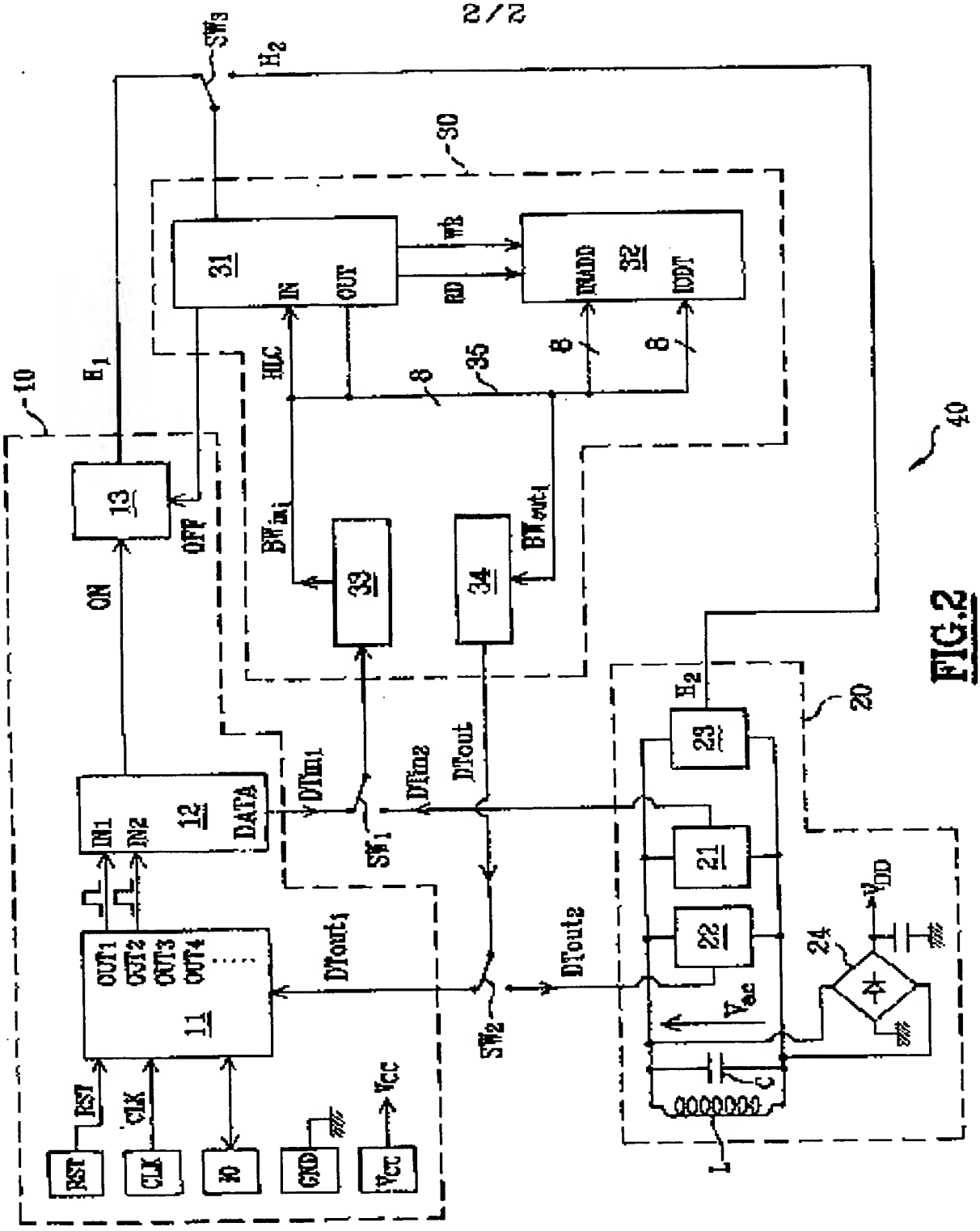

SW3
H2
30
31
IN
OUT
WR
RD
32
DATA
DDT
HLC
8
35
E1
10
13
ON
OFF
BWin1
33
34
BWout1
40
H2
20
23
DTin1
DTin2
DTout
12
IN1
IN2
DATA
SW1
21
22
24
VDD
OUT1
OUT2
OUT3
OUT4
11
DTout1
DTout2
SW2
Vac
C
RST
CLK
I/O
GND
Vcc

FIG.2